IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA, v. ANFERNEE CRUZ-FAJARDO, Defendant.	CRIMINAL CASE NO. 1:16-CR-14-TCB-LTW

MAGISTRATE JUDGE'S ORDER, FINAL REPORT AND RECOMMENDATION, AND ORDER CERTIFYING CASE READY FOR TRIAL

Pending before the Court are Defendant Anfernee Cruz-Fajardo's Motion to Compel Discovery (Doc. 40) and Supplemental Motion to Compel Discovery (Doc. 62). For the reasons outlined below, Defendant's Motions to Compel should be **DENIED**. (Docs. 40, 62). Also before the Court is Defendant's Unopposed Motion for Extension of Time to File Pretrial Motions and Request for Continuance of Pretrial Conference. Therein, Defendant requests an additional ten day continuance to file pretrial motions and for the pretrial conference. Defendant's Motion is **GRANTED NUNC PRO TUNC**. (Doc. 48).

MOTIONS TO COMPEL

Defendant's Motions to Compel concern whether the Government should be

compelled to give him the source code for software the Federal Bureau of Investigation ("FBI") surreptitiously deployed in an effort to ascertain the identities of individuals logging onto a website allegedly containing pornographic images so that the Government could ascertain their identities. Through the use of the software, Defendant was linked to the website.

I. BACKGROUND

A. The Target Website and the TOR Network

Between September 16, 2014, and February 3, 2015, FBI special agents in the District of Maryland investigated what they believed to be a child pornography website ("the Target Website"). (Def.'s Ex. A ¶ 11). The Target Website appeared to be a message board with the primary purpose of advertising and distributing child pornography. (Def.'s Ex. A ¶ 11).

The Target Website was accessible on TOR, which stands for "the onion router," a network that provides anonymity to internet users accessing the site. (Def.'s Ex. A ¶¶ 6-8; Gov't's Br. 2). The TOR protected users' privacy by bouncing their communications around a distributed network of relay computers run by volunteers around the world which masked the users' actual IP address, which could otherwise be used to identify users. (Def.'s Ex. A ¶ 8). In order to access the TOR network, users were required to install TOR software either by downloading an add-on to their web browser or by downloading the free browser bundle. (Def.'s Ex. A ¶¶ 7-8). The Target Website was a hidden service and did not reside on the traditional or open internet.

(Def.'s Ex. A ¶ 10). The Target Website could only be accessed via the TOR network; thus a user could not simply perform a Google search to locate the Target Website. (Def.'s Ex. A ¶ 10).

B. The FBI Obtains a Warrant to Install the Network Investigative Technique Affecting Users Logging Into the Target Website

In January 2015, the FBI, acting pursuant to a warrant, seized a copy of the TOR server which hosted the Target Website and ultimately seized control of the Target Website pursuant to a second warrant. (Def.'s Ex. A ¶¶ 28-30). Rather than shutting the website down, the FBI continued to operate it from a government-controlled computer server in Newington, Virginia, in an attempt to identify and prosecute users throughout the country. (Def.'s Ex. A ¶ 30; Def.'s Ex. C ¶ 11, 24). On February 20, 2015, the FBI obtained a warrant from a magistrate judge in the Eastern District of Virginia in order to deploy the "Network Investigative Technique" or "NIT" software onto the Target Website in the Eastern District of Virginia so that the FBI could investigate any user or administrator who logged into the Target Website. (Def.'s Ex. A ¶¶ 30-32). According to the FBI, the NIT operates as follows:

> In the normal course of operation, websites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. Under the NIT authorized by the warrant, the Target Website, which will be located in Newington, Virginia, in the Eastern District of Virginia, would augment that content with additional computer instructions. When a user's computer successfully downloads those instructions from the Target Website, . . . the instructions, which comprise the NIT, are designed to cause the user's "activating" computer to transmit certain information to a computer controlled by or known to the government. That information is described with particularity on the

> warrant . . . and the warrant authorizes obtaining no other information. The NIT will not deny the user of the "activating" computer access to any data or functionality of the user's computer.

(Def.'s Ex. A ¶ 33). Among other information, the NIT will provide the activating computer's IP address, the activating computer's host name, which is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, the activating computer's active operating system username, and the activating computer's Media Access Control ("MAC") address, which is an address from the computer's network adaptor. (Def.'s Ex. A ¶ 34).

C. The NIT Leads Law Enforcement to Defendant

According to the FBI, based on data obtained from logs on the Target Website, monitoring by law enforcement, and the deployment of the NIT, the FBI discovered that a user with the name "nonamenoname" browsed images of prepubescent girls involved in sexual activity on the Target Website on March 2, 2015. (Def.'s Ex. C ¶¶ 27-30). The NIT also determined the user's IP address and that the host name for the user nonamenoname was Heisenberg and the computer login was Anfernee. (Def.'s Ex. C ¶ 27). The FBI asserts that using publicly available websites, FBI special agents were able to determine that the user's IP address was operated by the internet service provider Comcast Cable. (Def.'s Ex. C ¶ 32). The FBI then served an administrative subpoena on Comcast Cable and learned as a result that Brandon Cannon was assigned to the IP address. (Def.'s Ex. C ¶ 32). On June 30, 2015, law enforcement observed a vehicle registered to Andrew Jackson Cannon parked outside of a Decatur apartment. (Def.'s

Ex. C ¶ 33). The FBI believed the vehicle was driven by Brandon Cannon. (Def.'s Ex. C ¶ 33). Based on this information, the FBI obtained a warrant on July 13, 2015, from a magistrate judge in the Northern District of Georgia for the search of the apartment. (Def.'s Ex. C, at 1). According to the Government, after agents subsequently searched the apartment, Defendant Cruz-Fajardo admitted that he had accessed the Target Website and exculpated his two roommates. (Gov't's Br. 6-7).

On January 12, 2016, a federal grand jury indicted Defendant Anfernee Cruz-Fajardo for knowingly receiving a visual depiction of a minor engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252(a)(2) and (b)(1) and for knowingly possessing at least one or more computers and computer storage devices which contained one or more visual depictions of minors engaged in sexually explicit conduct involving at least one prepubescent minor and at least one minor who had not attained twelve years of age in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2).

II. LEGAL ANALYSIS

Defendant contends that the Government should be compelled to produce certain aspects of the NIT source code, including (1) the unique identifier generator (which generates and saves a unique identifier which is used to link the server to an internet protocol address stored in the log file[1]); (2) exploit software which exploits a flaw in the

[1] The Government indicates that it will produce the unique identifier generator. (Doc. 45, at 16). Defendant responds that the Government did provide "a line of code that shows a unique identifier but it is limited in its usefulness" and "does not assist in determining whether or not the software was managed in the correct way." (Doc. 62, at 3). Defendant further states that his expert "cannot tell if it viewed the correct

user's computer that allows the NIT payload software to run and sends back the IP address and other data to the government; and (3) the data logger, which logs the data received from the NIT running on the user's computer.[2] Defendant argues the requested software is necessary to prepare for trial because Defendant needs to verify that the software operated in the manner the Government claims it does and that the software is able to do what the Government claims it can do. Defendant also argues that he may allege at trial that the FBI did not only send malware to his computer, but also child pornography, that the malware changed security settings on his computer leaving it vulnerable to hacking by other parties, and/or that the malware caused his computer to be used as a child-porn distribution hub. Defendant contends that he needs the software to confirm that the malware installed on Defendant's computer actually sent his true internet protocol address and other information to the FBI server. Defendant further argues he needs the NIT source code so his experts can verify that the NIT actually generates a unique identifier because if that component of the software did not work properly, the FBI's claim that it could unerringly link an IP address and a log-in would be disproved. Defendant also indicates that he needs to be able to confirm the FBI's

---

IP addresses, or if it was mistaken in the IP addresses it claims to have identified." (Doc. 62, at 3). The Government still indicates it provided the actual unique identifier generator to defense counsel. (Doc. 63, at 2).

[2] The Government responds that it has provided defense counsel and his expert with the instructions that the NIT source code sent to Defendant's computer and a demonstration of how the instructions collected information from Defendant's computer and what information was collected from the Defendant's computer based on those instructions. (Doc. 45, at 3-4).

chain of custody for the digital data between his computer, across the internet, and into storage on the FBI server, because if the data was sent unencrypted, the data could have been subject to tampering.

Under Rule 16 of the Federal Rules of Criminal Procedure, upon a defendant's request, the government "must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items . . . if the item is material to preparing the defense." Fed. R. Crim. P. 16(a)(1)(E)(I). The Government need not disclose items unless the defendant demonstrates that such items are material to the preparation of his defense. United States v. Jordan, 316 F.3d 1215, 1250 (11th Cir. 2003). The defendant must demonstrate materiality with more than a general description of the item or a conclusory argument that the requested item is material to the defense; the defendant must make a specific request for the item and an explanation of how it will be helpful to the defense. Jordan, 316 F.3d at 1250-51. "Helpful" in this respect means that the item is relevant to the preparation of the defense and not necessarily exculpatory. Jordan, 316 F.3d at 1251. That being said, the defendant must show "some indication that the pretrial disclosure of the item would . . . enable the defendant to significantly alter the quantum of proof in his favor." Jordan, 316 F.3d at 1251; United States v. Ross, 511 F.2d 757, 762 (5th Cir. 1975). Defendant has the burden of showing that his requested discovery is material. United States v. Buckley, 586 F.2d 498, 506 (5th Cir. 1978).

This Court finds that Defendant has failed to show that the requested source code is material. While Defendant lists a number of hypothetical ways in which the source code may be helpful: (1) the source code is necessary so that Defendant may confirm that the software could do what the Government says it can do; (2) the source code is necessary to determine whether the FBI only sent malware to his computer or whether the FBI also sent child pornography to his computer; (3) the source code is necessary to determine whether the malware changed security settings on his computer leaving it vulnerable to hacking by other parties or whether his computer was used as a child-porn distribution hub; (4) the source code is necessary to verify that the malware installed on Defendant's computer actually sent his true internet protocol address and other information to the FBI server; (5) the source code is necessary so that Defendant's expert can verify that the NIT actually generates a unique identifier because if that component of the software did not work properly, the FBI's claim that it could unerringly link an IP address and a log-in would be disproved; and (6) the source code is necessary to confirm the FBI's chain of custody for the digital data, because if the data was sent unencrypted, the data could have been subject to tampering. Although each of these bases for obtaining the source code could hypothetically lead to helpful information, such potential and hypothetical benefits are not enough to require the Government to produce the source code. Unlike broader civil discovery, which entitles a party "to discovery of any information sought if it appears 'reasonably calculated to lead to the discovery of admissible evidence,'" a criminal defendant is only entitled to

limited discovery. Degen v. United States, 517 U.S. 820, 825 (1996); United States v. Cerpas, 397 F. App'x 524, 528 (11th Cir. 2010). Before obtaining criminal discovery under Rule 16(a)(1)(E), a defendant must be able to show that the requested discovery can enable the defendant to significantly alter the quantum of proof in his favor. Jordan, 316 F.3d at 1251; Ross, 511 F.2d at 762. Here, Defendant fails to do so because he presents no factual basis supporting the notion that obtaining the source code would lead to information which would exonerate him or shed doubt on whether the NIT properly functioned with respect to him. FBI Special Agent Daniel Alfin, whose duties include the investigation of individuals using various types of technology to produce, distribute, and trade child pornography and who has completed all stages of FBI cyber training, states that he has tested the NIT on a computer under his control and observed that it does not disable the security firewall, make changes to the security settings, or leave residual malware on the computer under his control. (Decl. of Special Agent Daniel Alfin, hereinafter "Alfin Decl.," ¶ 9). Additionally, as the Government points out, Defendant has been given portions of the software, has been given the unique identifier generator, has been provided with the instructions that the NIT source code sent to Defendant's computer, and has been given a demonstration of how the instructions collected information from the Defendant's computer. Yet, Defendant has provided no factual basis suggesting, for instance, that the NIT affected his security settings, that there was an issue with chain of custody, that the NIT sent child pornography to his computer, or that the NIT did not send his true internet protocol address and other

information to the FBI server. Because Defendant's speculation, without more is insufficient to show materiality, Defendant is not entitled to the source code. See United States v. Gaver, No. 3:16-cr-88, 2017 WL 1134814, at *3-4 (S.D. Ohio Mar. 27, 2017) (refusing to compel production of the source code because Defendant's speculative arguments failed to demonstrate that source code was material to the defense); United States v. Owens, No. 16-CR-38-JPS, 2016 WL 7351270, at *6 (E.D. Wis. Dec. 19, 2016) (rejecting defendant's arguments that the source code was material because it would aid him in evaluating potential defensive theories about the chain of custody with respect to his data, about whether the NIT operated as the government indicated it would in its warrant application, about whether the NIT permitted the government to change the security settings on his computer, and about whether third party hacking occurred because Defendant did not present any expert analysis indicating that his theories had any factual support); United States v. McLamb, No. 2:16cr92, — F. Supp. 3d —, 2016 WL 6963046, at *8 (E.D. Va. Nov. 28, 2016) (denying motion to compel exploit source code and unique identifier generator on the grounds that defendant did not prove materiality because defendant only offered hypothetical situations in which the requested software could be helpful); United States v. Jean, No. 5:15-CR-50087-001, 2016 WL 6886871, at *7 (W.D. Ark. Nov. 22, 2016) (concluding that defendant's hypothetical arguments as to why he needed the source code were insufficient to establish that the source code would be material to his defense).

Defendant also requests that the Government inform him of the total number of

pictures and videos that were downloaded from the target website while it was controlled by the FBI and the number of visitors during that time. Likewise, Defendant seeks documents and records relating to the Department of Justice's review, approval, and supervision of the Target Website's operation. Defendant contends that such information is relevant to his Motion to Dismiss the Indictment. This Court has already reviewed the Motion to Dismiss the Indictment and has determined that even if the facts supporting the Motion are as described by Defendant, dismissal is unwarranted. Thus, Defendant is not entitled to further discovery to develop his Motion. Additionally, the Government responds that it has already answered Defendant's questions regarding the number of visitors to the site while the FBI was running it and the number of pictures and videos that were downloaded by users during the same period. (Doc. 45, at 3). Based on the Government's statement, it is the understanding of this Court that Defendant has already been provided this information. Accordingly, Defendant's Motion to Compel should be **DENIED**.

CONCLUSION

Based on the foregoing reasons, this Court **RECOMMENDS** that Defendant's Motion to Compel Discovery (Doc. 40) and Supplemental Motion to Compel Discovery (Doc. 62) be **DENIED**. (Docs. 40, 62). Defendant's Unopposed Motion for Extension of Time to File Pretrial Motions and Request for Continuance of Pretrial Conference is **GRANTED NUNC PRO TUNC**. (Doc. 48). There are no further motions or problems pending before the undersigned to prevent the scheduling of this case for trial.

Therefore, this case is **CERTIFIED READY FOR TRIAL**.[3]

SO ORDERED AND REPORTED AND RECOMMENDED this 8 day of June, 2017.

/s/Linda T. Walker
LINDA T. WALKER
UNITED STATES MAGISTRATE JUDGE

[3] Although Defendant's Motion to Exclude or Suppress Defendant's Statements (Doc. 28) has been submitted to this Court, this Court deferred the matter to the District Court (Doc. 31) because Jackson v. Denno, 378 U.S. 368 (1964) issues predominate in the Motion.

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA, v. ANFERNEE CRUZ-FAJARDO, Defendant.	CRIMINAL CASE NO. 1:16-CR-14-TCB-LTW

ORDER FOR SERVICE OF FINAL REPORT AND RECOMMENDATION

Attached is the report and recommendation of the United States Magistrate Judge made in this action in accordance with 28 U.S.C. § 636 and N.D. Ga. CrR. 59(2)(a). Let the same be filed and a copy, together with a copy of this Order, be served upon counsel for the parties.

Pursuant to 28 U.S.C. § 636(b)(1), within fourteen (14) days after service of this order, each party may file written objections, if any, to the Report and Recommendation. Pursuant to Title 18, United States Code, Section 3161(h) (1) (D), (H), **the above-referenced fourteen (14) days allowed for objections is EXCLUDED from the computation of time under the Speedy Trial Ac, whether or not the objections are actually filed.** If objections to this Report and Recommendation are filed, the Clerk is **DIRECTED** to **EXCLUDE** from the computation of time all time between the filing

of the Report and Recommendation and the submission of the Report and Recommendation, along with any objections, responses and replies thereto, to the District Judge. 18 U.S.C. § 3161(h)(1)(D), (H); Henderson v. United States, 476 U.S. 321, 331 (1986); United States v. Mers, 701 F.2d 1321, 1337 (11th Cir. 1983). Should objections be filed, they shall specify with particularity the alleged error or errors made (including reference by page number to the transcript if applicable) and shall be served upon the opposing party. The party filing objections will be responsible for obtaining and filing the transcript of any evidentiary hearing for review by the district court. If no objections are filed, the report and recommendation may be adopted as the opinion and order of the district court and any appellate review of factual findings will be limited to a plain error review. United States v. Slay, 714 F.2d 1093 (11th Cir. 1983), cert. denied, 464 U.S. 1050 (1984).

The Clerk is directed to submit the report and recommendation with objections, if any, to the District Court after expiration of the above time period.

SO ORDERED, this 8 day of June, 2017.

/s/Linda T. Walker
LINDA T. WALKER
UNITED STATES MAGISTRATE JUDGE